Listing of Claims:

1. – 4. (Cancelled)

5. (Currently Amended) A security apparatus system comprising:

a verifier apparatus for determining an authorization to process protected material to facilitate an assessment by the verifier apparatus of the physical proximity of the source of a response, based on an assessment of actual response times associated with one or more responses received from an unknown second source to one or more non-scheduled requests issued from a first source to the unknown second source,

a timer apparatus operably coupled to the verifier apparatus for measuring response times between a non-scheduled request for content from a first source and a response from the unknown second source,

a storage medium for storing the actual response times for limiting subsequent access of [[the]] unauthorized users or notifying an external source of the unauthorized users,

wherein each of the one or more non-scheduled requests issued from the first source comprise a request for access to randomly selected source information from the unknown second source,

wherein the assessment of the response times forms an assessment of whether the one or more responses were communicated locally to the verifier or via a network connection; and

wherein the assessment of the one or more responses performed by the verifier comprises: continuously requesting randomly selected source information from the unknown source unit until a statistically observable difference from the expected response time of a local source is detected, and

wherein the one or more responses are stored for limiting subsequent access of the unauthorized users or notifying an external source of the unauthorized users.

6. – 8. (Cancelled)

9. -13. (Cancelled)

14. (New) The security apparatus system of claim 5, further comprising a renderer for receiving a plurality of data items corresponding to a data set, and for producing therefrom a rendering corresponding to a select data item.

15. (New) The security apparatus system of claim 14, wherein the renderer is configured to preclude the rendering corresponding to the select data item in dependence upon whether other data items of the plurality of data items are available to the renderer.

16. (New) The security apparatus system of claim 5, wherein the verifier apparatus precludes the rendering based at least in part on an assessment of the response times.

17. (New) The security apparatus system of claim 5, wherein the assessment of the response times corresponds to a determination of whether the other data items are located in physical proximity to the renderer.

18. (New) The security apparatus system of claim 5, wherein the verifier is configured to randomly select the other data items.

19. (New) The security apparatus system of claim 5, wherein the verifier is configured to form the assessment based on at least one of: an average of the response times, a comparison of the response times to one or more threshold times, and a statistical test based on the response times.

20. (New) A method of verifying the authenticity of requested data, the method comprising:

requesting by a processor, data from an unknown remote access device that a user is attempting to render on a rendering device;

verifying by a verifier module that the access device is able to provide data different from the requested data based on a temporal proximity measure;

denying the request from being completed by the verifier module in the case where the verification fails; and

otherwise granting the request by the verifier module in the case where the verification succeeds.

21. (New) The method of claim 1, wherein the verification step further comprises:

directing the renderer by the verifier module to request said different data; and

determining by the verifier module that the different data is not available from the unknown remote access device.

22. (New) The method of claim 1, wherein the verification step further comprises:

measuring response times from requests made by the rendering device to the unknown remote access device, wherein the response time is between a non-scheduled request from the rendering device and a response from the unknown remote access device;

assessing the response times to form an assessment of whether one or more responses were communicated locally to the verifier or via a network connection;

23. (New) The method of claim 22, wherein the one or more requests are for randomly selected source information from the unknown remote access device.

24. (New) The method of claim 23, wherein the one or more requests are made until a statistically observable difference from an expected response time of a local source is detected.

25. (New) The method of claim 20, further comprising a step of storing the actual response times to either limit subsequent access by unauthorized users or notifying an external source of unauthorized users.